

Notice of Allowability

Application No.

09/770,877

Examiner

Minh Dieu Nguyen

Applicant(s)

LOTSPIECH ET AL.

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to April 26, 2005.
2. ☒ The allowed claim(s) is/are 1, 3-5, 8-23, 26, 28, 30-42, 44-45, 48-60, 65-67, 69-81, 83-88, and 95-98.
3. ☒ The drawings filed on 16 September 2002 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

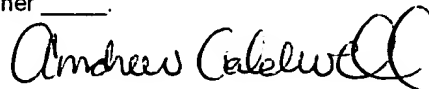
* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
(a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
(b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date 1/26/01; 9/16/02; 9/23/04
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with John Rogitz on 5/6/2005.

2. The application has been amended as follows:

Please amend the claims as specified on page 3.

1. (currently amended) A method for broadcast encryption, comprising:
 assigning each user in a group of users respective private information I_u ;
 selecting at least one session encryption key K ;
 partitioning users not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having associated subset keys L_{i1}, \dots, L_{im} ; [and]
 encrypting the session key K with the subset keys L_{i1}, \dots, L_{im} to render m encrypted versions of the session key K ;
partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree, wherein each subset S_{i1}, \dots, S_{im} includes all leaves in a subtree rooted at some node v_i , at least each node in the subtree being associated with a respective subset key, wherein content is provided to users in at least one message defining a header, and the header includes at most $r \cdot \log(N/r)$ subset keys and encryptions, wherein r is the number of users in the revoked set R and N is the total number of users.
2. (canceled).
3. (currently amended) The method of Claim [2]1, wherein the tree is a complete binary tree.
4. (original) The method of Claim 1, further comprising using private information I_u to decrypt the session key.

5. (original) The method of Claim 4, wherein the act of decrypting includes using information i_j such that a user belongs to a subset S_{ij} , and retrieving a subset key L_{ij} using the private information of the user.
6. (canceled).
7. (canceled).
8. (currently amended) The method of Claim [6]1, wherein each user must store $\log N$ keys, wherein N is the total number of users.
9. (currently amended) ~~The method of Claim 6~~ A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information I_u ;
selecting at least one session encryption key K ;
partitioning users not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having associated subset keys L_{i1}, \dots, L_{im} ; [and]
encrypting the session key K with the subset keys L_{i1}, \dots, L_{im} to render m encrypted versions of the session key K ;
partitioning the users into groups S_1, \dots, S_w , wherein " w " is an integer, and the groups establish subtrees in a tree, wherein each subset S_{i1}, \dots, S_{im} includes all leaves in a subtree rooted at some node v_i , at least each node in the subtree being associated with a respective subset key, wherein content is provided to

users in at least one message, and wherein each user processes the message using at most $\log \log N$ operations plus a single decryption operation, wherein N is the total number of users.

10. (currently amended) The method of Claim [6]1, wherein the revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

11. (currently amended) The method of Claim [2]1, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i .

12. (currently amended) ~~The method of Claim 11~~ A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information I_u ;
selecting at least one session encryption key K ;
partitioning users not in a revoked set R into disjoint subsets S_1, \dots, S_m having associated subset
keys L_1, \dots, L_m ;
encrypting the session key K with the subset keys L_1, \dots, L_m to render m encrypted versions of the
session key K ;

partitioning the users into groups S_1, \dots, S_w , wherein " w " is an integer, and the groups establish
subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at least one
associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are
not in the subtree rooted at some other node v_j that descends from v_i , wherein content is provided to users

in at least one message defining a header, and the header includes at most $2r-1$ subset keys and encryptions, wherein r is the number of users in the revoked set R .

13. (currently amended) ~~The method of Claim 11~~ A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information I_u ;
selecting at least one session encryption key K ;
partitioning users not in a revoked set R into disjoint subsets S_1, \dots, S_m having associated subset keys L_1, \dots, L_m ;
encrypting the session key K with the subset keys L_1, \dots, L_m to render m encrypted versions of the session key K ;
partitioning the users into groups S_1, \dots, S_w , wherein " w " is an integer, and the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i , wherein each user must store $.5\log^2 N + .5\log N + 1$ keys, wherein N is the total number of users.

14. (currently amended) ~~The method of Claim 11~~ A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information I_u ;
selecting at least one session encryption key K ;
partitioning users not in a revoked set R into disjoint subsets S_1, \dots, S_m having associated subset keys L_1, \dots, L_m ;

encrypting the session key K with the subset keys L_{i1}, \dots, L_{im} to render m encrypted versions of the session key K;

partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i , wherein content is provided to users in at least one message, and wherein each user processes the message using at most $\log N$ operations plus a single decryption operation, wherein N is the total number of users.

15. ~~The method of Claim 11~~ A method for broadcast encryption, comprising:

assigning each user in a group of users respective private information I_u ;

selecting at least one session encryption key K;

partitioning users not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having associated subset keys L_{i1}, \dots, L_{im} ;

encrypting the session key K with the subset keys L_{i1}, \dots, L_{im} to render m encrypted versions of the session key K;

partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i , wherein the revoked set R defines a spanning tree, and wherein the method includes:

initializing a cover tree T as the spanning tree;

iteratively removing nodes from the cover tree T and adding nodes to a cover until the cover tree T has at most one node.

16. ~~The method of Claim 11~~ A method for broadcast encryption, comprising:

assigning each user in a group of users respective private information L_u ;

selecting at least one session encryption key K;

partitioning users not in a revoked set R into disjoint subsets S_1, \dots, S_m having associated subset keys L_{i1}, \dots, L_{im} ;

encrypting the session key K with the subset keys L_{i1}, \dots, L_{im} to render m encrypted versions of the session key K;

partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i , wherein each node has at least one label possibly induced by at least one of its ancestors, and wherein each user is assigned labels from all nodes hanging from a direct path between the user and the root but not from nodes in the direct path.

17. (original) The method of Claim 16, wherein labels are assigned to subsets using a pseudorandom sequence generator, and the act of decrypting includes evaluating the pseudorandom sequence generator.

18. (currently amended) ~~The method of Claim 1~~ A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information I_u ;
selecting at least one session encryption key K ;
partitioning users not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having associated subset
keys L_{i1}, \dots, L_{im} ; and
encrypting the session key K with the subset keys L_{i1}, \dots, L_{im} to render m encrypted versions of the
session key K , wherein content is provided to users in at least one message having a header including a
cryptographic function E_L , and the method includes prefix-truncating the cryptographic function E_L .

19. (currently amended) The method of Claim [2]1, wherein the tree includes a root and plural nodes, each node having an associated key, and wherein each user is assigned keys from all nodes in a direct path between a leaf representing the user and the root.

20. (currently amended) ~~The method of Claim 1~~ A method for broadcast encryption, comprising:
assigning each user in a group of users respective private information I_u ;
selecting at least one session encryption key K ;
partitioning users not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having associated subset
keys L_{i1}, \dots, L_{im} ; and
encrypting the session key K with the subset keys L_{i1}, \dots, L_{im} to render m encrypted versions of the
session key K , wherein content is provided to users in at least one message defining plural portions, and
each portion is encrypted with a respective session key.

21. (currently amended) A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer, comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render encrypted versions of the session key; [and]

logic means for sending the encrypted versions of the session key in a header of the message to plural stateless receivers, wherein logic means provide content to receivers in at least one message, and wherein each receiver processes the message using at most $\log \log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

22. (original) The computer program device of Claim 21, further comprising:

logic means for partitioning receivers not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having associated subset keys L_{i1}, \dots, L_{im} .

23. (original) The computer program device of Claim 22, further comprising logic means for partitioning the users into groups S_1, \dots, S_w , wherein " w " is an integer, and the groups establish subtrees in a tree.

24. (original) The computer program device of Claim 21, further comprising logic means for using private information I_u to decrypt the session key.

25. (original) The computer program device of Claim 24, wherein the means for decrypting includes logic means for using information i_j such that a receiver belongs to a subset S_{ij} , and retrieving a key L_{ij} from the private information of the receiver.

26. (original) The computer program device of Claim 23, wherein each subset S_{i1}, \dots, S_{im} includes all leaves in a subtree rooted at some node v_i , at least each node in the subtree being associated with a respective subset key.

27. (canceled).

28. (original) The computer program device of Claim 26, wherein each receiver must store $\log N$ keys, wherein N is the total number of receivers.

29 (canceled).

30. (original) The computer program device of Claim 26, wherein the revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

31. (original) The computer program device of Claim 23, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i .

32. (currently amended) ~~The computer program device of Claim 31~~ A computer program device,
comprising:

a computer program storage device including a program of instructions usable by a computer,

comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render
encrypted versions of the session key;

logic means for sending the encrypted versions of the session key in a header of the message to
plural stateless receivers;

logic means for partitioning receivers not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having
associated subset keys L_{i1}, \dots, L_{im} ;

logic means for partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the
groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at
least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i
that are not in the subtree rooted at some other node v_j that descends from v_i , wherein logic means provide
content to receivers in at least one message defining a header, and the header includes at most $2r-1$ subset
keys and encryptions, wherein r is the number of receivers in the revoked set R.

33. (currently amended) ~~The computer program device of Claim 31~~ A computer program device,
comprising:

a computer program storage device including a program of instructions usable by a computer,

comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render
encrypted versions of the session key;

logic means for sending the encrypted versions of the session key in a header of the message to
plural stateless receivers;

logic means for partitioning receivers not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having
associated subset keys L_{i1}, \dots, L_{im} ;

logic means for partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the
groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at
least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i
that are not in the subtree rooted at some other node v_j that descends from v_i , wherein each receiver must
store $.5\log^2 N + .5\log N + 1$ keys, wherein N is the total number of receivers.

34. (currently amended) ~~The computer program device of Claim 31~~ A computer program device,
comprising:

a computer program storage device including a program of instructions usable by a computer,
comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render
encrypted versions of the session key;

logic means for sending the encrypted versions of the session key in a header of the message to
plural stateless receivers;

logic means for partitioning receivers not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having
associated subset keys L_{i1}, \dots, L_{im} ;

logic means for partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the
groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at
least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i
that are not in the subtree rooted at some other node v_j that descends from v_i , wherein logic means provide
content to receivers in at least one message, and wherein each receiver processes the message using at
most log N operations plus a single decryption operation, wherein N is the total number of receivers.

35. (currently amended) ~~The computer program device of Claim 31~~ A computer program device,
comprising:

a computer program storage device including a program of instructions usable by a computer,

comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render encrypted versions of the session key;

logic means for sending the encrypted versions of the session key in a header of the message to plural stateless receivers;

logic means for partitioning receivers not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having associated subset keys L_{i1}, \dots, L_{im} ;

logic means for partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i , wherein the revoked set R defines a spanning tree, and wherein ~~(original)~~ The the computer program device includes:

logic means for initializing a cover tree T as the spanning tree; and

logic means for iteratively removing nodes from the cover tree T and adding nodes to a cover until the cover tree T has at most one node.

36. (original) The computer program device of Claim 35, wherein logic means assign labels to receivers using a pseudorandom sequence generator, and the labels induce subset keys.

37. (original) The computer program device of Claim 36, wherein the means for decrypting includes evaluating the pseudorandom sequence generator.

38. (currently amended) ~~The computer program device of Claim 21~~ A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer,

comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render encrypted versions of the session key; and

logic means for sending the encrypted versions of the session key in a header of the message to plural stateless receivers, wherein logic means provide content to receivers in at least one message having a header including a cryptographic function E_L , and ~~(original) The~~ the computer program device includes logic means for prefix-truncating the cryptographic function E_L .

39. (original) The computer program device of Claim 23, wherein the tree includes a root and plural nodes, each node having an associated key, and wherein logic means assign each receiver keys from all nodes in a direct path between a leaf representing the receiver and the root.

40. (currently amended) ~~The computer program device of Claim 21~~ A computer program device,
comprising:

a computer program storage device including a program of instructions usable by a computer,
comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render
encrypted versions of the session key; and

logic means for sending the encrypted versions of the session key in a header of the message to
plural stateless receivers, wherein logic means provide content to receivers in at least one message
 defining plural portions, and each portion is encrypted with a respective session key.

41. (currently amended) A computer programmed with instructions to cause the computer to execute
 method acts including:

encrypting broadcast content; [and]

sending the broadcast content to plural stateless receivers and to at least one revoked receiver such
 that each stateless receiver can decrypt the content and the revoked receiver cannot decrypt the content;

partitioning the users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish
subtrees in a tree, wherein each subset S_1, \dots, S_{im} includes all leaves in a subtree rooted at some node v_i , at
least each node in the subtree being associated with a respective subset key, wherein content is provided to
receivers in at least one message defining a header, and the header includes at most $r \cdot \log(N/r)$ subset keys

and encryptions, wherein r is the number of receivers in the revoked set R and N is the total number of receivers.

42. (original) The computer of Claim 41, wherein the method acts further comprise:
 assigning each receiver in a group of receivers respective private information I_u ;
 selecting at least one session encryption key K ;
 partitioning all receivers not in a revoked set R into disjoint subsets S_{i1}, \dots, S_{im} having associated subset keys L_{i1}, \dots, L_{im} ; and
 encrypting the session key K with the subset keys L_{i1}, \dots, L_{im} to render m encrypted versions of the session key K .

43. (canceled).

44. (currently amended) The computer of Claim [43]41, wherein the tree is a complete binary tree.

44. (canceled).

45. (currently amended) The computer of Claim [44]49, wherein the act of decrypting undertaken by the computer includes using information i_j such that a receiver belongs to a subset S_{ij} , and retrieving a key L_{ij} using the private information of the receiver.

46. (canceled).

47. (canceled).

48. (currently amended) The computer of Claim [46]41, wherein each receiver must store $\log N$ keys, wherein N is the total number of receivers.

49. (currently amended) ~~The computer of Claim 46~~ A computer programmed with instructions to cause the computer to execute method acts including:

encrypting broadcast content;

partitioning users into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree, wherein each subset S_{i1}, \dots, S_{im} includes all leaves in a subtree rooted at some node v_i , at least each node in the subtree being associated with a respective subset key;

sending the broadcast content to plural stateless receivers and to at least one revoked receiver such that each stateless receiver can decrypt the content and the revoked receiver cannot decrypt the content, wherein content is provided to receivers in at least one message, and wherein each receiver processes the message using at most $\log \log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

50. (currently amended) The computer of Claim [46]41, wherein the revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

51. (original) The computer of Claim 41[43], wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i .

52. (original) The computer of Claim 51, wherein content is provided to receivers in at least one message defining a header, and the header includes at most $2r-1$ subset keys and encryptions, wherein r is the number of receivers in the revoked set R .

53. (original) The computer of Claim 51, wherein each receiver must store $.5\log^2 N + .5\log N + 1$ keys, wherein N is the total number of receivers.

54. (original) The computer of Claim 51, wherein content is provided to receivers in at least one message, and wherein each receiver processes the message using at most $\log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

55. (original) The computer of Claim 51, wherein the revoked set R defines a spanning tree, and wherein the method acts undertaken by the computer further include:

initializing a cover tree T as the spanning tree;

iteratively removing nodes from the cover tree T and adding nodes to a cover until the cover tree

T has at most one node.

56. (original) The computer of Claim 55, wherein the computer assigns node labels to receivers from the tree using a pseudorandom sequence generator.

57. (original) The computer of Claim 56, wherein the act of decrypting undertaken by the computer includes evaluating the pseudorandom sequence generator.

58. (currently amended) ~~The computer of Claim 41~~ A computer programmed with instructions to cause the computer to execute method acts including:

encrypting broadcast content;

sending the broadcast content to plural stateless receivers and to at least one revoked receiver such that each stateless receiver can decrypt the content and the revoked receiver cannot decrypt the content, wherein content is provided to receivers in at least one message having a header including a cryptographic function E_L , and the method acts undertaken by the computer include prefix-truncating the cryptographic function E_L .

59. (currently amended) ~~The computer of Claim 41~~ A computer programmed with instructions to cause the computer to execute method acts including:

encrypting broadcast content;

sending the broadcast content to plural stateless receivers and to at least one revoked receiver such that each stateless receiver can decrypt the content and the revoked receiver cannot decrypt the content,

wherein content is provided to receivers in at least one message defining plural portions, and each portion is encrypted by the computer with a respective session key.

60. (original) The method of Claim 11, wherein each node has plural labels with each ancestor of the node inducing a respective label, and wherein each user is assigned labels from all nodes hanging from a direct path between the user and the root but not from nodes in the direct path.

61-64. (canceled).

65. (previously presented) A receiver of content, comprising:

means for storing respective private information I_u ;

means for receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content; and

means for obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content, wherein the receiver receives content in at least one message defining a header, and the header includes at most $r \cdot \log(N/r)$ subset keys and encryptions, wherein r is the number of receivers in a revoked set R and N is the total number of receivers.

66. (original) The receiver of Claim 65, wherein the receiver is partitioned into one of a set of groups S_1, \dots, S_w , wherein " w " is an integer, and the groups establish subtrees in a tree defining nodes and leaves.

67. (original) The receiver of Claim 66, wherein subsets S_{i1}, \dots, S_{im} derived from the set of groups S_1, \dots, S_w define a cover.

68. (canceled).

69. (original) The receiver of Claim 67, wherein the receiver must store $\log N$ keys, wherein N is the total number of receivers.

70. (previously presented) A receiver of content, comprising:

means for storing respective private information I_u ;

means for receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content; and

means for obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content, wherein the receiver receives content in at least one message defining a header, and wherein the receiver processes the message using at most $\log \log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

71. (original) The receiver of Claim 67, wherein a revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

72. (original) The receiver of Claim 67, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i .

73. (previously presented) A receiver of content, comprising:

means for storing respective private information I_u ;

means for receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content; and

means for obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content, wherein the receiver receives content in a message having a header including at most $2r-1$ subset keys and encryptions, wherein r is the number of receivers in the revoked set R .

74. (previously presented) A receiver of content, comprising:

means for storing respective private information I_u ;

means for receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content; and

means for obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content, wherein the receiver must store $.5\log^2 N + .5\log N + 1$ keys, wherein N is the total number of receivers.

75. (previously presented) A receiver of content, comprising:

means for storing respective private information I_u ;

means for receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content; and

means for obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content, wherein content is provided to the receiver in at least one message, and wherein the receiver processes the message using at most $\log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

76. (original) The receiver of Claim 72, wherein the receiver decrypts the subset key by evaluating a pseudorandom sequence generator.

77. (previously presented) A receiver of content, comprising:

a data storage storing respective private information I_u ;

a processing device receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content, the processing device obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content, wherein the receiver receives content in at least one message defining a header, and wherein the receiver processes the message using at most $\log \log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

78. (original) The receiver of Claim 77, wherein the receiver is partitioned into one of a set of groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree.

79. (original) The receiver of Claim 78, wherein subsets S_{i1}, \dots, S_{im} derived from the set of groups S_1, \dots, S_w define a cover.

80. (original) The receiver of Claim 79, wherein the receiver receives content in at least one message defining a header, and the header includes at most $r \cdot \log(N/r)$ subset keys and encryptions, wherein r is the number of receivers in a revoked set R and N is the total number of receivers.

81. (original) The receiver of Claim 79, wherein the receiver must store $\log N$ keys, wherein N is the total number of receivers.

82. (canceled).

83. (original) The receiver of Claim 79, wherein one revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

84. (original) The receiver of Claim 79, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i .

85. (original) The receiver of Claim 84, wherein the receiver receives content in a message having a header including at most $2r-1$ subset keys and encryptions, wherein r is the number of receivers in the revoked set R .

86. (original) The receiver of Claim 84, wherein the receiver must store $.5\log^2 N + .5\log N + 1$ keys, wherein N is the total number of receivers.

87. (original) The receiver of Claim 84, wherein content is provided to the receiver in at least one message, and wherein the receiver processes the message using at most $\log N$ operations plus a single decryption operation, wherein N is the total number of receivers.

88. (original) The receiver of Claim 84, wherein the receiver decrypts the subset key by evaluating a pseudorandom sequence generator.

89-94 (canceled).

95. (currently amended) The computer of Claim [42]41, wherein the act of partitioning is undertaken by a system computer in a system of receivers separate from the system computer.

96. (currently amended) The computer of Claim [42]41, wherein the act of partitioning is undertaken by a receiver computer.

97. (original) The receiver of Claim 67, wherein the receiver derives the subsets in the cover.
98. (previously presented) The computer of Claim 41, wherein the method acts include using private information I_u to decrypt the session key.

Art Unit: 2137

Allowable Subject Matter

3. The examiner's amendment indicates the amendments to claims 1, 3, 8-16, 18-21, 32-35, 38, 40-41, 44-45, 48-50, 58-59 and 95-96 and the cancellation of claims 2, 6-7, 27, 29, 43, 44, 46-47, 61-64, 68, 82 and 89-94.

4. Claims 1, 3-5, 8-23, 26, 28, 30-42, 44-45, 48-60, 65-67, 69-81, 83-88 and 95-98 are allowed.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
5/9/05



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER